(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Publication number : **0 516 682 B1**

(12) EUROPEAN PATENT SPECIFICATION

(45) Date of publication of patent specification : **21.06.95 Bulletin 95/25**

(51) Int. Cl.[6] : **G06F 11/00,** G06F 12/14

(21) Application number : **91904667.2**

(22) Date of filing : **20.02.91**

(86) International application number : **PCT/GB91/00261**

(87) International publication number : **WO 91/13403 05.09.91 Gazette 91/21**

(54) METHOD AND APPARATUS FOR CONTROLLING ACCESS TO AND CORRUPTION OF INFORMATION IN COMPUTER SYSTEMS.

(30) Priority : **21.02.90 GB 9003890**

(43) Date of publication of application : **09.12.92 Bulletin 92/50**

(45) Publication of the grant of the patent : **21.06.95 Bulletin 95/25**

(84) Designated Contracting States : **DE FR GB SE**

(56) References cited :
FR-A- 2 629 231
US-A- 3 742 458
US-A- 3 827 029
US-A- 4 215 400
Siemens Microcomputer Components: Data Catalog, 1986/87, München, pages 539, 554-565
Intel, Introduction to the iAPX 286, 1985, Santa Clara, page 3-20 to 3-21
H-P. Messmer, PC-Hardwarebuch, 1993, Addison-Wesley,Bonn, Paris, page 160 and 485-496

(73) Proprietor : **Killean, Reginald Cameron Gordon**
Linwood, Kirkbank Road
Burntisland, Fife KY39 9HZ (GB)
Proprietor : **Robb, David Shepherd Stewart**
30A Shore Road
Anstruther, Fife (GB)

(72) Inventor : **KILLEAN, Reginald**
Linwood,
Kirkbank Road
Burntisland KY3 9HZ (GB)
Inventor : **ROBB, David**
30A Shore Road
Anstruther, Fife (GB)
Inventor : **WHITE, Norman, Jackson**
96 Muirs, Kinross
Tayside KY13 7AZ (GB)

(74) Representative : **Ede, Eric et al**
Fitzpatricks,
4 West Regent Street
Glasgow G2 1RS, Scotland (GB)

EP 0 516 682 B1

Description

The present invention relates to methods and apparatus for preventing the corruption or destruction of data in computer systems, and is particularly concerned with the detection and containment of hostile programs such as "virus" programs within computer systems. The word "virus", which has become a well-known term in the art, will be used herein as a generic name for all hostile programs.

There is an increasing problem with computer viruses which are introduced into computer systems by clandestine means with consequences of varying degrees of seriousness from minor inconvenience to the system user, to complete destruction of data or disablement of the system. The propagation of viruses can be controlled by controlling the operations which can be performed on particular data or classes of data. However, proposals to date for implementing such classification methods rely on a high degree of user discipline, and/or hardware modification of computers and/or hard disks, and/or software modification of the operating system, and/or knowledge of virus signatures.

It is an object of the present invention to obviate or mitigate the aforesaid disadvantages.

It is a further object of the present invention to provide a method of, and apparatus for, virus detection and containment capable of implementation on a computer system using: a 'standard' version of a given computer operating system; a 'standard' computer capable of operation using such an operating system; and 'standard' computer devices.

In the sense used hereinbefore, the word 'standard' means that which would be routinely purchased from manufacturers of these devices, without special modification.

The invention described herein may aptly be described as a 'Supervisor' ie. an arrangement which controls read, write and format operations performed on data on a storage medium of a computer system. While it is true that an operating system supervises the transfer and storage of all data within a computer system it is also true that a virus can be introduced and can circumvent this supervision if the computer is used with doubtful or unlicensed software. This allows a potential virus to replicate itself, to change, damage or delete data, and even to make the whole system inoperable.

It is, therefore, a further object of the present invention to provide an additional level of supervision which addresses the above circumstances. The invention specifically limits the damage a virus can cause and protects certain existing data areas.

It should, however, be stressed that there exists a hierarchy of potential virus infection ranging from innocent usage of infected software, even after precautions have been followed, through to deliberate sabotage of a system. There is ultimately no defence against this latter situation, given that computer systems are designed to respond to human inputs. The present invention would not claim to prevent this situation either. What it does do is to provide a framework within which a viral attack may be detected and contained. It, therefore, allows the user a mechanism for protection of his files. Starting from a virus-free position, it permits a way of introducing further software or modifications to existing software which, if infected, would corrupt only part of the user's existing system.

According to a first aspect of the invention there is provided a method of controlling access to and modification of information stored on a storage medium forming part of a computer system comprising:

dividing information stored on the storage medium into a plurality of non-overlapping partitions, including a boot partition and a plurality of general partitions, each of the partitions being further divided into a plurality of sectors, any designated subset of the general partitions being active at any given time when the computer system is in use,

characterised by,

providing supervising means (a Supervisor) separate of a central processing unit (CPU) of the computer system and made inaccessible to the user for controlling the performance of read, write and format operations upon the information stored on the storage medium so as to allow, restrict or prevent such operations depending upon the type of information stored within a sector and type and status of the partition within which the sector is located,

the supervising means causing a reset to be required of the computer system should an attempt be made to perform a prohibited read, write or format operation, said reset causing memory to be cleared and the operating system to be loaded.

In the preferred embodiment of the invention, read operations are allowed on any information in the boot partition, but an attempt to write to or format the boot partition causes a system reset.

Notwithstanding this constraint, write operations to certain designated bytes within the boot partition could be allowed under the direct control of the Supervisor, dependent for example on the requirements of the computer operating system.

As part of the invention, the boot sectors of the storage medium are treated as part of the boot partition,

irrespective of the position of the starting sector of the boot partition as may be defined by the disk operating system.

Preferably also, reading of any operating system information sectors or user-generated information sectors in an active general partition is allowed, writing to such user-generated information sectors is allowed, and writing to such operating system information sectors is restricted such that an attempt to modify the size or boundaries of the partition causes a system reset.

Preferably also, only the reading of information from operating system sectors of inactive general partitions is allowed, and an attempt to perform any other read, write or format operation on such partitions is either denied or causes a system reset.

According to a second aspect, the invention provides an apparatus for controlling access to and modification of information stored on a storage medium of a computer system, the information on the storage medium being divided into a plurality of non-overlapping partitions, including a boot partition and a plurality of general partitions, each partition being further divided into a plurality of sectors, any designated subset of the general partitions being active at any given time when the computer system is in use, **characterised in that** the apparatus comprises a supervising means (a Supervisor) separate of a central processing unit (CPU) of the computer system for controlling the performance of read, write or format operations stored on the storage medium so as to allow, restrict or prevent such operations depending upon the type of information stored within a sector and the type and status of the partition within which the sector is located wherein, in use, the supervising means causes a reset to be required of the computer system should an attempt be made to perform a prohibited read, write or format operation.

The invention may provide hardware means or firmware means or a combination of both adapted to be incorporated into an existing system so as to implement the method defined above. This may be in the form of packages which can be mounted within a system or as stand-alone units.

This invention preferably uses a second processor which is made inaccessible to the user and to the virus. This processor's sole purpose is to supervise all data transfer between and within sub-divisions of the device or devices placed under its control.

The processor's function is, therefore, to impose restrictions on certain operations dependent on certain criteria, namely, the data type, the source and destination of the data in question and possibly the user of the machine. The actual information stored does not, however, play any role in the decision process.

A partition, in the case of a storage device such as a hard disk, is considered itself to be a device or a subdivision of a device. In the case of a fileserver the equivalent partition is a node on the network or sub-division of a node. The supervising processor uses these definitions in its decision making process.

The Supervisor may be implemented on a printed circuit board as an expansion card to be inserted into the computer system.

Further details of various aspects of the invention will now be discussed in the following description of an embodiment of the invention, given by way of example only, with reference to the accompanying drawings which are:

Fig. 1 a schematic block diagram of a hardware arrangement embodying a Supervisor according to the present invention; and

Fig. 2 a schematic circuit diagram of an actual embodiment of the Supervisor of Fig. 1.

In the following description the storage medium given as an example is a hard disk and the system is an IBM PC.

In order to understand the background to the invention it is necessary to give a brief review of certain organisational aspects of DOS, an operating system applicable to 'IBM-compatible' personal computers. A hard disk may be divided by the user into several logically discrete areas called partitions. Each of these partitions is made up of logically consecutive sectors. Within each partition the starting sectors and a number of additional sectors contain, amongst other information, the starting and ending sector addresses of the partition and the information essential for finding the sectors in which a given file is located within the partition. Partitions cannot overlap. Under DOS, the first physical sector of the hard disk also contains essential information regarding the partition geometry. The invention treats this sector as an integral part of the boot partition.

In order to give an understanding of a Supervisor according to the invention, a general description will first be given of the function of the Supervisor, whether it is implemented in hardware, firmware or a combination of both. A specific description of an embodiment of a 'Supervisor' will then be given with reference to Figs. 1 and 2.

In general terms the invention relates to the control that the Supervisor exerts over partitions of a storage medium, in this example a hard disk. The user is encouraged to make active use of separate partitions for separate applications programs. The Supervisor stores partition information including, for each partition, the sector bounds and addresses of those sectors containing Operating System information (OS-sectors) and those con-

taining User Information (UI-sectors).

The user may use several partitions on the disk. All these partitions, save for one, are treated in an equivalent way by the Supervisor. In essence, they are kept independent of each other, but may, if required, be linked. The special partition is the boot partition, and may be termed the Unique partition or U-partition. The U-partition will contain, at least, the sectors for booting the hard disk and the DOS operating system files. It could also be used to store other files which are 'read-only' and known to be virus-free.

At any point in time, any one or, if allowed, more of the remaining partitions (general partitions) will be 'Active' and may be termed the A-partition(s). The remaining 'other' partitions may then be termed O-partitions. It will be the user's choice as to which partition or partitions become active, either by deliberate pre-selection at boot or by automatic activation as a result of the first write to OS-sectors or read/write to UI-sectors of a partition other than the U-partition.

The functions of the Supervisor are defined in Table 1. There are three typical disk commands: Read, Write and Format. Table 1 shows how the Supervisor controls these commands depending upon the type and status of the relevant partition and sector.

TABLE 1

PARTITION TYPE	SECTOR TYPE	READ COMMAND	WRITE COMMAND	FORMAT COMMAND
U-PARTITION	OS-SECTORS	ALLOW	RESET*	RESET
U-PARTITION	UI-SECTORS	ALLOW	RESET*	RESET
A-PARTITION	OS-SECTORS	ALLOW	RESTRICTED	ALLOW
A-PARTITION	UI-SECTORS	ALLOW	ALLOW	ALLOW
O-PARTITION	OS-SECTORS	ALLOW	RESET	RESET
O-PARTITION	UI-SECTORS	RESET/WARNING	RESET	RESET

* excepting designated bytes, if any.

The interpretation of Table 1 is as follows:-

(a) At any time, all files in the U-partition may be read. Any attempt to write or format will be detected and result in a reset.

(b) Within an A-partition, reading, writing and formatting is allowed to all files. Note that, where permitted, writing to OS-sectors is termed 'restricted' which means that attempts to modify the partition basic geometry (bounds, size) would be detected by the Supervisor and result in a reset of the computer.

(c) The only command permitted on an O-partition is that of reading OS-sectors. All others will either cause a reset or be denied. In particular, UI-sectors may not be read since the 'read' action could contain an implied 'execute'.

When the Supervisor applies a reset, this in turn results in a cold re-boot of the computer. This reset is critical as memory must be cleared in order to prevent a virus from remaining intact in memory.

Should a virus exist in a program, it can only become active when that program is read from the disk and then executed. By definition, since the U-partition is virus-free, that program could only be stored in a current A-partition and any attempt by the virus to corrupt, that is write to, any file in other partitions would be detected and prohibited. The Supervisor would initiate a reset which would clear memory, load the operating system and bring the computer to a virus-free condition.

Prior to this action, the Supervisor will set a register to an appropriate value and write a message to the disk which, on completion of the re-boot, will be read by the computer and used to define one of a set of non-corruptible messages held in a ROM (Read Only Memory).

This will be sent to the screen of a Video Display Unit of the computer system giving the user information on the reason for the reset and thus warning him of an attempt to write illegally, which could be a signal that a virus is present in the previous A-partition.

Clearly, a virus can be introduced into the hard disk. It can replicate itself and corrupt files, but only in the partition in which it was loaded. Thus, the virus can be contained and it can be detected when it tries to spread outwith the partition in which it resides.

All of the above protection constraints take effect when the Supervisor is in so-called 'supervised' mode. This is the normal default mode when the system is booted from the hard disk.

Initially, however, it is necessary to place the Supervisor in so-called 'unsupervised' mode, in order to allow the setting up of the hard disk in terms of its partitions, and this is achieved by booting from a DOS floppy disk. Once the initial set-up of the hard disk has been achieved, a Password has to be chosen and the Supervisor will only permit itself to be placed in unsupervised mode again when booted from a floppy disk if the same Password is correctly entered on the keyboard.

It will be recognised that the unsupervised mode is potentially dangerous. However, it is necessary to be able to implement this mode for legitimate operations including system set-up and maintenance. Provision is provided for the Password to be changed when the system is put in unsupervised mode.

It is clear from the foregoing that the invention treats the partitions as though they were complete logical disks. At any one time therefore, a current A-partition (or designated set of A-partitions), is to all intents and purposes a hard disk in its own right.

In hardware form the Supervisor may reside in the back plane of the computer and will look like (or be) a modified hard disk adaptor card with the additional capability of resetting the computer. Its hardware will control the hard disk bidirectionally, the intelligence of the Supervisor will be derived from a microprocessor, RISC processor or transputer with the controlling program resident in ROM.

A typical example of the use of the Supervisor would include the addition of a hard disk drive, using a SCSI (Small Computer Systems Interface) interface to a personal computer with no SCSI initiator capability. In this case the Supervisor would be part of the SCSI adaptor card, slotted in the back plane of the computer, which would be needed in any case for interfacing the drive to the computer. Another example would be that of a computer with an existing SCSI output port, to which a SCSI drive is coupled. Then the Supervisor would be a (smaller) card attached to the SCSI connector port to which the drive cable would attach.

Alternatively, in the firmware form the Supervisor could simply consist of modifications to the hard disk firmware and to the firmware of a suitable SCSI adaptor card. The Supervisor would then intercept SCSI signals, but would be designated to be effectively transparent to either the host or the drive.

Whether in hardware or firmware form, the Supervisor will have sufficient volatile memory to hold the DOS operating system parameters that define the partition structure.

Referring now to Figure 1 there is shown a block diagram of a hardware arrangement suitable for implementing the Supervisor. The Supervisor provides a typical hard disk adaptor card interface 10 to a mother board of a person computer (PC) or the like, and Read Only Memory (ROM) 12 containing an appropriate BIOS (Basis Input/Output System) driver for operation of the hard disk.

The Supervisor hardware embodying the invention includes a microprocessor 14 and a transceiver 16,

which allow the PC restricted access to a SCSI 18 such that the PC cannot directly select or arbitrate for the disk drive or issue commands over the SCSI interface 18. These operations can be performed only by the Supervisor microprocessor 14, which communicates bidirectionally with the PC using status in/out ports 20 and 22.

Communication between the microprocessor 14 and the SCSI interface 18 takes place via the bidirectional ports of a second transceiver 24. The Supervisor also includes its own Read Only Memory (ROM) 26, holding a Supervisor Operating System and a control program, and Random Access Memory (RAM) 28, which is a scratch memory used to hold parameters. Reset logic 30 is also provided, and is used for clearing the PC memory if and when an attempt is made to perform an operation prohibited by the Supervisor.

Referring to Figure 2 there is shown a schematic diagram of an actual embodiment of the invention with the integers numbered identically to those of Fig. 1.

The embodiment of Fig. 2 further includes the following components: Gate Array Logic (GAL) devices G1-G5; buffers B1, B2; and flip-flops 74,1(1), 74,1(2), 74,2(1) and 74,2(2).

The function of these components is as follows. G1 maps the ROM BIOS into the IBM memory map, and also provides tristate connection of the output of flip-flop 74,2(2) to the IBM data bus.

G2 provides access by the IBM to a subset of the SCSI controller's internal registers by mapping them into the IBM I/O space. G2 further provides pseudo-DMA decoding logic for data transfer to/from the SCSI controller, and maps a flag, ie. flip-flop 74,2(2) and latch P1 into the IBM I/O space.

G3 multiplexes between the Supervisor and IBM address buses, to the SCSI controller address bus.

G4 multiplexes between the Supervisor and IBM control lines, to the SCSI controller. G4 also enables either (but never both) transceivers T1, T2, and includes logic for possible wait state during data transfers between the IBM and the SCSI controller G5 maps all ports in the Supervisor I/O space: Latches P1, P2, SCSI reset line and flip-flops 74,1(2) and 74,2(2). G5 further maps ROM into the Supervisor memory map, and provides tristate connection of output of flip-flop 74,2(2) to the Supervisor data bus.

The buffers B1, B2 ensure that there can be only one gate draining current from the IBM Backplane for each of the address, IOR and IOW lines.

Flip-flop 74,1(1) divides the clock frequency by two and squares up the pulses. Dependent on the output of 74,1(2), either the IBM has access (restricted) or the Supervisor has access, to the SCSI controller.

74,2(1) provides part of the timing for wait state generation during SCSI date transfer, while 74,2(2) is a flag to indicate that a data byte has been sent by the IBM for the attention of the Supervisor.

The components of the embodiment of Fig. 2 are as follows. GAL's G1-G5 are of the type SGS Thomson GAL 16V8-15ns; flip-flops 74,1(1), 74,1(2), 74,2(1) and 74,2(2) are of the type 74ALS74; buffers B1, B2 are 74ALS244's; latches P1, P2 are 74ALS373's; transceivers T1, T2 are 74F245's; the processor 14 is a Zilog Z84C50 (10MHz); the ROM 12 a 2764A (8k x 8); and the SCSI controller 18 a NCR 5380.

Inspection of Fig. 2 clearly shows that a virus can never interfere with the Supervisor microprocessor 14 since it is only able to fetch executable code from its own ROM 26.

A more detailed description of the embodiment of the Supervisor shown in Fig. 2 is not given herein, as this would be within the normal understanding of a person skilled in the art.

Other options within the scope of the invention are possible. For example in firmware form, the Supervisor could substantially be resident on the hard disk itself. It could also handle hard disks which have interfaces other than SCSI, eg. AT or ESDI.

In general the principles of the embodiment of the invention hereinbefore described apply to the coupling of any hard disk to any computer by any interface. For example, the invention cold equally be applied to the popular Apple Macintosh range of personal computers which use an operating system different from DOS. Furthermore, it should be appreciated that application also exists for multi-user fileservers, in which case the Supervisor on the fileserver will require to be aware of which user (terminal) is using which fileserver partition so that it knows which computer to reset if an illegal request is made.

As will be seen from the foregoing, the invention provides a means of protecting computer systems against virus infection and may be implemented in hardware or firmware with no modification of an existing hardware or operating system. Further, it requires virtually no active participation by the user in order to be effective. Devices which could be protected by the invention include, for example, hard disk drives, floppy disk drives, optical disk drives, tape drives, file servers and networks.

Claims

1. A method of controlling access to and modification of information stored on a storage medium forming part of a computer system comprising:

dividing information stored on the storage medium into a plurality of non-overlapping partitions, including a boot partition and a plurality of general partitions, each of the partitions being further divided into a plurality of sectors, any designated subset of the general partitions being active at any given time when the computer system is in use

characterised by,

providing supervising means (12, 14, 16, 18, 20, 22, 24, 26, 28, 30) separate of a central processing unit (CPU) of the computer system and made inaccessible to the user for controlling the performance of read, write and format operations upon the information stored on the storage medium so as to allow, restrict or prevent such operations depending upon the type of information stored within a sector and type and status of the partition within which the sector is located,

the supervising means causing a reset to be required of the computer system should an attempt be made to perform a prohibited read, write or format operation, said reset causing memory to be cleared and the operating system to be loaded.

2. A method as claimed in claim 1, **characterised in that** read operations are allowed on any information in the boot partition, but an attempt to write or format the boot partition causes a system reset.

3. A method as claimed in claims 1 or 2, **characterised in that** boot sectors of the storage medium are considered to be part of the boot partition, irrespective of the position of the starting sector of the boot partition as may be defined by the storage medium operating system.

4. A method as claimed in claims 1 to 3 inclusive, **characterised in that** reading of any operating system information sectors or user-generated information sectors in an active general partition is allowed, writing to such user-generated information sectors is allowed, and writing to such operating system information sectors is restricted such that an attempt to modify the size or boundaries of the partition causes a system reset.

5. A method as claimed in any of claims 1 to 4 inclusive, **characterised in that** only the reading of information from operating system sectors of inactive general partitions is allowed, and an attempt to perform any other read, write or format operations on such partitions is either denied or causes a system reset.

6. A method as claimed in any preceding claim, **characterised in that** the restriction or prevention of the performance of read, write and format operations can be removed to allow setup or maintenance of the storage medium and thereafter reinstated.

7. A method as claimed in any of claims 1 to 6 inclusive, **characterised in that** the storage medium is any one of a hard disk, a floppy disk, an optical disk or a tape.

8. A method as claimed in any of claims 1 to 6 inclusive, **characterised in that** the storage medium is a fileserver, and the computer system is a local area network, and which user computer is using which partition of the fileserver is determined such that an attempt by a user computer to perform a prohibited operation causes a reset to be required of the user computer.

9. An apparatus for controlling access to and modification of information stored on a storage medium of a computer system, the information on the storage medium being divided into a plurality of non-overlapping partitions, including a boot partition and a plurality of general partitions, each partition being further divided into a plurality of sectors, any designated subset of the general partitions being active at any given time when the computer system is in use, **characterised in that** the apparatus comprises a supervising means separate of a central processing unit (CPU) of the computer system and made inaccessible to the user for controlling the performance of read, write or format operations depending upon the information stored on the storage medium so as to allow, restrict or prevent such operations depending upon the type of information stored within a sector and the type and status of the partition within which the sector is located wherein, in use, the supervising means causes a reset to be required of the computer system should an attempt be made to perform a prohibited read, write or format operation, said reset causing memory to be cleared and the operating system to be loaded.

10. An apparatus as claimed in claim 9, **characterised in that** the apparatus provides hardware means adapted to be incorporated into the computer system.

11. An apparatus as claimed in claim 9, **characterised in that** the apparatus provides firmware means adapted to be incorporated into the computer system.

12. An apparatus as claimed in claim 9, **characterised in that** the apparatus provides a combination of both hardware and firmware means, both being adapted to be incorporated into the computer system.

13. An apparatus as claimed in any of claims 9, **characterised in that** there is provided a processor (14) which is made inaccessible to a user and to any virus and which supervises all data transfers between and within sub-divisions of the storage medium or storage media placed under its control.

Patentansprüche

1. Verfahren, um den Zugriff auf und eine Veränderung von Informationen zu kontrollieren, die in einem Speichermedium gespeichert sind, das Teil eines Computersystems ist, mit den Schritten:

   es wird die in dem Speichermedium gespeicherten Informationen in eine Vielzahl nicht überlappender Partitions aufgeteilt, zu denen eine Bootpartition sowie eine Anzahl allgemeiner Partitions gehört, wobei ferner jede Partition in eine Vielzahl von Sektoren aufgeteilt wird, und jedes benannte Subset der allgemeinen Partitions zu jeder beliebigen Zeit, zu der das Computersystem in Gebrauch ist, aktiv ist, dadurch gekennzeichnet,

   daß Überwachungsmittel (12, 14, 16, 18, 20, 22, 24, 26, 28, 30) bereitgestellt werden, die von der zentralen Verarbeitungseinheit (CPU) des Computersystems getrennt und für den Benutzer unzugänglich gemacht werden, um die Ausführung von Lese-, Schreib- und Formatierungsoperationen an den in dem Speichermedium gespeicherten Informationen zu kontrollieren, um so abhängig von dem in einem Sektor gespeicherten Informationstyp und von dem Typ und dem Zustand der Partition, innerhalb der sich der Sektor befindet, solche Operationen zuzulassen, einzuschränken oder zu verhindern,

   und daß erforderlichenfalls die Überwachungsmittel ein Rücksetzen des Computersystems bewirken, falls ein Versuch gemacht werden sollte, eine verbotene Lese-, Schreibe- oder Formatierungsoperation durchzuführen, wobei das Zurücksetzen bewirkt, daß der Speicher bereinigt und das Betriebssystem geladen wird.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß die Leseoperationen für alle Informationen in der Bootpartition gestattet sind, jedoch ein Versuch in die Bootpartition zu schreiben oder sie zu formatieren, ein Rücksetzen des Systems verursacht.

3. Verfahren nach den Ansprüchen 1 oder 2, dadurch gekennzeichnet, daß die Bootsektoren in dem Speichermedium als Teil der Bootpartition angesehen werden, unabhängig von der Position des Startsektors der Bootpartition, wie sie durch das Betriebssystem für das Speichermedium definiert ist.

4. Verfahren nach den Ansprüchen 1 bis 3, dadurch gekennzeichnet, daß das Lesen beliebiger Informationssektoren des Betriebssystems oder beliebiger durch Benutzer erzeugter Informationssektoren in der aktiven allgemeinen Partition zulässig ist, daß das Schreiben in solchen vom Benutzer erzeugten Informationssektoren zulässig ist und daß das Schreiben in solche Informationssektoren des Betriebssystems in der Weise beschränkt ist, daß ein Versuch, die Größe oder die Grenzen der Partition zu verändern, ein Rücksetzen des Systems bewirkt.

5. Verfahren nach einem der Ansprüche 1 bis 4 einschließlich, dadurch gekennzeichnet, daß lediglich das Lesen von Informationen aus den Sektoren des Betriebssystems aus inaktiven allgemeinen Partitions zulässig ist und ein Versuch, jede andere Lese-, Schreib- oder Formatierungsoperation in solchen Partitions durchzuführen, entweder abgelehnt wird oder ein Rücksetzen des Systems bewirkt.

6. Verfahren nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, daß die Beschränkung oder Verhinderung Lese-, Schreib- oder Formatierungsoperationen auszuführen, aufgehoben werden kann, um die Einstellung oder Wartung des Speichermdiums zu ermöglichen, und daß diese sodann wieder in Kraft gesetzt wird.

7. Verfahren nach einem der Ansprüche 1 bis 6 einschließlich, dadurch gekennzeichnet, daß das Speichermedium eine Harddisk, eine Floppydisk, eine Optical-disk oder ein Band ist.

8. Verfahren nach einem der Ansprüche 1 bis 6 einschließlich, dadurch gekennzeichnet, daß das Speichermedium ein Fileserver und das Computersystem ein lokales Netzwerk ist und daß die Festlegung welcher Benutzercomputer welche Partition des Fileservers verwendet derart getroffen ist, daß ein Versuch seitens eines Benutzercomputers, eine verbotene Operation auszuführen, bewirkt, daß erforderlichenfalls der Benutzercomputer zurückgesetzt wird.

9. Vorrichtung, um den Zugriff auf und eine Veränderung von Informationen zu kontrollieren, die in einem Speichermedium gespeichert sind, das Teil eines Computersystems ist, wobei die in dem Speichermedium gespeicherten Informationen in eine Vielzahl nicht überlappender Partitions aufgeteilt wird, zu denen eine Bootpartition sowie eine Anzahl allgemeiner Partitions gehört, wobei ferner jede Partition in eine Vielzahl von Sektoren aufgeteilt wird, und jedes benannte Subset der allgemeinen Partitions zu jeder beliebigen Zeit, zu der das Computersystem in Gebrauch ist, aktiv ist, dadurch gekennzeichnet,

daß die Vorrichtung Überwachungsmittel aufweist, die von der zentralen Verarbeitungseinheit (CPU) des Computersystems getrennt und für den Benutzer unzugänglich gemacht sind, um die Ausführung von Lese-, Schreib- und Formatierungsoperationen an den in dem Speichermedium gespeicherten Informationen zu kontrollieren, um so abhängig von dem in einem Sektor gespeicherten Informationstyp und von dem Typ und dem Zustand der Partition, innerhalb der sich der Sektor befindet, solche Operationen zuzulassen, einzuschränken oder zu verhindern, wobei im Gebrauch erforderlichenfalls die Überwachungsmittel ein Rücksetzen des Computersystems bewirken, falls ein Versuch gemacht werden sollte, eine verbotene Lese-, Schreibe- oder Formatierungsoperation durchzuführen, und das Zurücksetzen bewirkt, daß der Speicher bereinigt und das Betriebssystem geladen wird.

10. Vorrichtung nach Anspruch 9, dadurch gekennzeichnet, daß sie Hardwaremittel aufweist, die so gestaltet sind, daß diese in das Computersystem inkorporierbar sind.

11. Vorrichtung nach Anspruch 9, dadurch gekennzeichnet, daß sie Firmwaremittel aufweist, die so gestaltet sind, daß diese in das Computersystem inkorporierbar sind.

12. Vorrichtung nach Anspruch 9, dadurch gekennzeichnet, daß sie ein Kombination aus Hardware- und Firmwaremitteln aufweist, die beide so gestaltet sind, daß diese in das Computersystem inkorporierbar sind.

13. Vorrichtung nach einem der Ansprüche 9 bis 12, dadurch gekennzeichnet, daß ein Prozessor (14) vorgesehen ist, der für Benutzer und beliebige (Computer-)Viren unzugänglich gemacht ist und daß der gesamte Datentransfer zwischen und innerhalb von Untereinheiten des Speichermediums oder der Speichermedien unter seine Kontrolle gestellt ist.

Revendications

1. Procédé pour commander l'accès et modifier des informations enregistrées sur un support de stockage faisant partie d'un système informatique comprenant :

la division d'informations enregistrées sur le support de stockage en une pluralité de partitions non chevauchantes, comprenant une partition d'initialisation et une pluralité de partitions générales, chacune des partitions étant en outre divisée en une pluralité de secteurs, n'importe quel sous-ensemble désigné des partitions générales étant actif à n'importe quel instant donné lorsque le système informatique est utilisé, caractérisé par

la fourniture de moyens de supervision (12, 14, 16, 18, 20, 22, 24, 26, 28, 30) indépendants d'une unité centrale de traitement (CPU) du système informatique et rendus inaccessibles à l'utilisateur pour commander l'exécution d'opérations de lecture, d'écriture et de formatage sur les informations enregistrées sur le support de stockage afin d'autoriser, de limiter ou d'interdire de telles opérations en fonction du type d'informations enregistrées dans un secteur et du type et de l'état de la partition dans laquelle le secteur est situé,

les moyens de supervision provoquant une réinitialisation à requérir du système informatique si une tentative d'exécution d'une opération interdite de lecture, d'écriture ou de formatage est effectuée, ladite réinitialisation provoquant le vidage de la mémoire et le chargement du système d'exploitation.

2. Procédé selon la revendication 1, caractérisé en ce que des opérations de lecture sont autorisées sur n'importe quelle information dans la partition d'initialisation, une tentative d'écriture ou de formatage de la partition d'initialisation provoquant cependant une réinitialisation du système.

3. Procédé selon la revendication 1 ou 2, caractérisé en ce que des secteurs d'initialisation du support de stockage sont considérés comme une partie de la partition d'initialisation, indépendamment de la position du secteur de démarrage de la partition d'initialisation telle qu'elle peut être définie par le système d'exploitation du support de stockage.

4. Procédé selon l'une quelconque des revendications 1 à 3, caractérisé en ce que la lecture de n'importe quel secteur d'informations du système d'exploitation ou secteur d'informations généré par l'utilisateur dans une partition générale active est autorisée, l'écriture dans de tels secteurs d'informations générés par l'utilisateur est autorisée, et l'écriture dans de tels secteurs d'informations du système d'exploitation est limitée de telle sorte qu'une tentative pour modifier la taille ou les limites de la partition provoque une réinitialisation du système.

5. Procédé selon l'une quelconque des revendications 1 à 4, caractérisé en ce que seule la lecture d'informations provenant de secteurs du système d'exploitation de partitions générales inactives est autorisée, et une tentative pour exécuter n'importe quelle autre opération de lecture, d'écriture ou de formatage sur de telles partitions est refusée ou bien provoque une réinitalisation du système.

6. Procédé selon l'une quelconque des revendications précédentes, caractérisé en ce que la limitation ou l'interdiction de l'exécution d'opérations de lecture, d'écriture et de formatage peut être annulée pour permettre la configuration ou la maintenance du support de stockage et être ensuite rétablies.

7. Procédé selon l'une quelconque des revendications 1 à 6, caractérisé en ce que le support de stockage est n'importe quel disque dur, disquette, disque optique ou bande.

8. Procédé selon l'une quelconque des revendications 1 à 6, caractérisé en ce que le support de stockage est un serveur de fichiers, et le système informatique est un réseau local, et tel ordinateur d'utilisateur utilisant telle partition du serveur de fichiers est déterminé de telle sorte qu'une tentative par un ordinateur d'utilisateur d'exécuter une opération interdite provoque une réinitialisation à requérir de l'ordinateur de l'utilisateur.

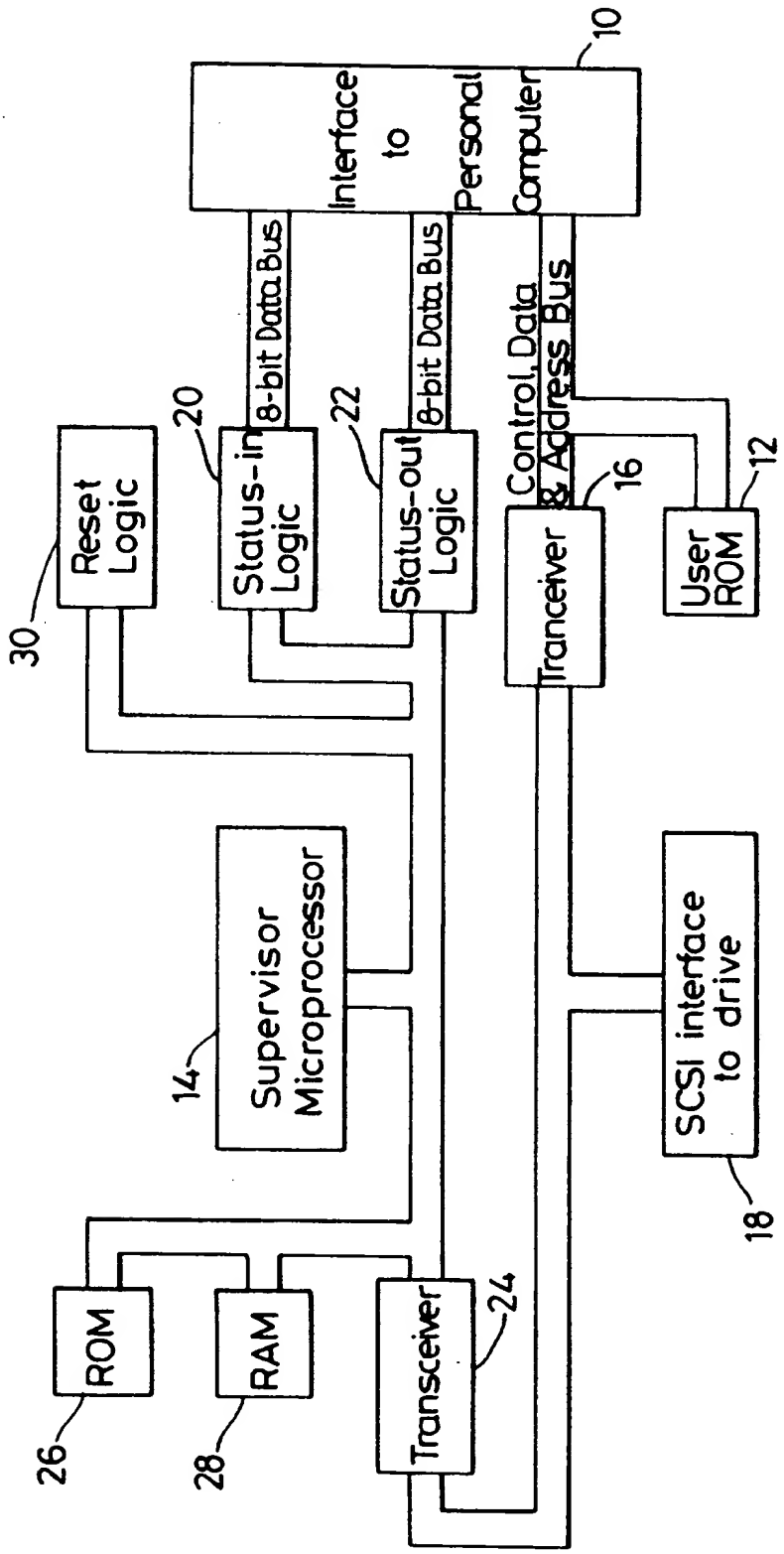
9. Appareil pour commander l'accès et la modification d'informations enregistrées sur un support de stockage d'un système informatique, les informations du support de stockage étant divisées en une pluralité de partitions non chevauchantes, comprenant une partition d'initialisation et une pluralité de partitions générales, chaque partition étant en outre divisée en une pluralité de secteurs, n'importe quel sous-ensemble désigné des partitions générales étant actif à n'importe quel instant donné lorsque le système informatique est utilisé, caractérisé en ce que l'appareil comprend des moyens de supervision indépendants d'une unité centrale de traitement (CPU) du système informatique et rendus inaccessibles à l'utilisateur pour commander l'exécution d'opérations de lecture, d'écriture ou de formatage en fonction des informations enregistrées sur le support de stockage afin d'autoriser, de limiter ou d'interdire de telles opérations en fonction du type d'informations enregistrées dans un secteur et du type et de l'état de la partition dans laquelle le secteur est situé en ce que, en utilisation, les moyens de supervision provoquent une réinitialisation à requérir du système informatique si une tentative d'exécution d'une opération interdite de lecture, d'écriture ou de formatage est effectuée, ladite réinitialisation provoquant le vidage de la mémoire et le chargement du système d'exploitation.

10. Appareil selon la revendication 9, caractérisé en ce que l'appareil fournit des moyens matériels adaptés pour être incorporés dans le système informatique.

11. Appareil selon la revendication 9, caractérisé en ce que l'appareil fournit des moyens de microprogrammation adaptés pour être incorporés dans le système informatique.

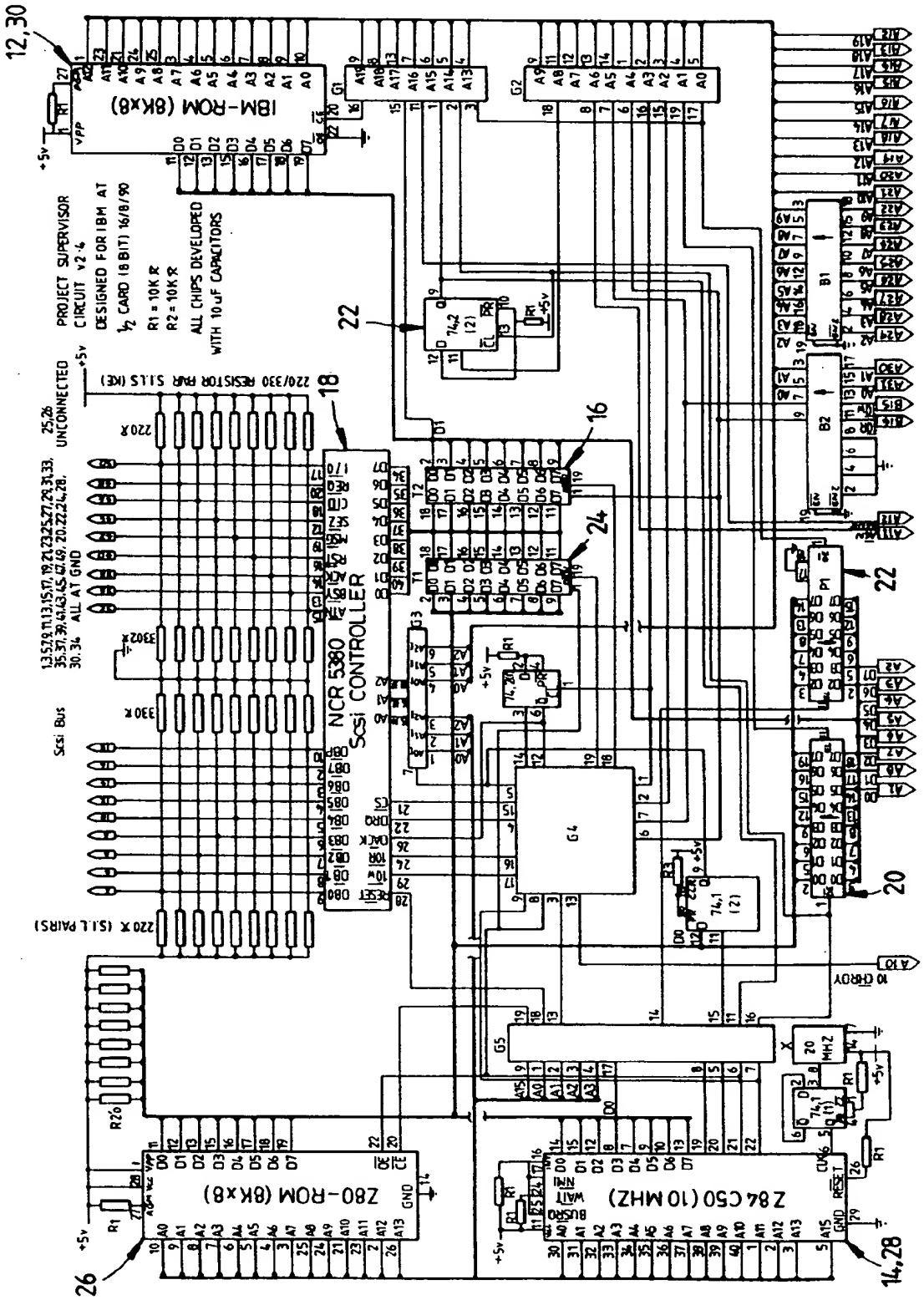
12. Appareil selon la revendication 9, caractérisé en ce que l'appareil fournit une combinaison de moyens matériels et de microprogrammation, tous deux adaptés pour être incorporés dans le système informatique.

13. Appareil selon l'une quelconque des revendications 10 à 12, caractérisé en ce qu'un processeur (14) est proposé lequel est rendu inaccessible à un utilisateur et à n'importe quel virus et qui supervise tous les transferts de données entre et à l'intérieur des subdivisions du support de stockage ou des supports de stockage placés sous son contrôle.



SUPERVISOR BLOCK DIAGRAM

Fig. 1


12,30
IBM-ROM (8K x 8)
PROJECT SUPERVISOR CIRCUIT v2·4
DESIGNED FOR IBM AT
½ CARD (8 BIT) 16/8/90
R1 = 10K Ω
R2 = 10K Ω
ALL CHIPS DEVELOPED WITH 10µF CAPACITORS
25,26 UNCONNECTED
1,3,5,7,9,11,13,15,17,19,21,23,25,27,29,31,33, 35,37,39,41,43,45,47,49, 20,22,24,28, 30,34 ALL AT GND
220/330 RESISTOR PAR SILS (KE)
220 R
330 R
220 X (SIL PAIRS)
Scsi Bus
NCR 5380 Scsi CONTROLLER
Z80-ROM (8K x 8)
Z 84 C50 (10 MHZ)
20 MHZ
10 CHROY
18
16
24
22
20
26
14,28